|  |
| --- |
| **ANNEXE N°2 AU MARCHE PUBLIC N°25-2546**  relatif à la protection des données à caractère personnel |

|  |
| --- |
| **A - Identification du pouvoir adjudicateur** |

**CENTRE HOSPITALIER UNIVERSITAIRE DE TOULOUSE**

**Hôtel-Dieu Saint-Jacques**

**2, rue Viguerie TSA 80035**

**31059 TOULOUSE cedex 9**

*SIRET CHU : 26310012500016*

|  |  |
| --- | --- |
| **Nom, prénom et adresse du DPO :**  *(délégué à la protection des données du CHU de Toulouse ainsi que des établissements membres du G.H.T. Haute-Garonne et Tarn Ouest)* | **Madame Charlène SEGURA**  Hôtel Dieu Saint-Jacques  2 rue Viguerie  31059 TOULOUSE CEDEX  [dpo@chu-toulouse.fr](mailto:dpo@chu-toulouse.fr) |

|  |
| --- |
| **B - Identification du Titulaire du marché ou de l’accord-cadre** |

|  |  |
| --- | --- |
| **Nom de l’entreprise ou de la société :**  *(mandataire en cas de groupement)* |  |
| **Adresse siège social :** |  |
| **Adresse de l’établissement**  **qui exécutera la prestation** *(si différente du siège)***:** |  |
| **Téléphone :** |  |
| **Télécopie :** |  |
| **Courriel :** |  |
| **Numéro de SIRET :** |  |

|  |  |
| --- | --- |
| **Nom, prénom et adresse du DPO :**  *(délégué à la protection des données du Titulaire, s’il en a désigné un)* |  |

|  |
| --- |
| **C - Objet du marché ou de l’accord-cadre** |

**◼** Objet du marché ou de l’accord-cadre : **ACQUISITION, INSTALLATION, MISE EN SERVICE ET MAINTENANCE D’UN INCUBATEUR DE CULTURE EMBRYONNAIRE TIME LAPSE AINSI QUE LA FOURNITURE DE PIECES DETACHEES, D’ACCESSOIRES, SOUS-ENSEMBLES, CONSOMMABLES, UPDATES ET FORMATIONS ASSOCIES**

**◼** Numéro et intitulé du lot : **Non alloti**

**◼** Date de notification du ou de l’accord-cadre :

**◼** Durée d’exécution du marché ou de l’accord-cadre (reconductions comprises) : **48 mois**

**◼** Montant initial du marché ou de l’accord-cadre : **400 000 € HT**

|  |
| --- |
| **D - Objet** |

**◼ Article 1 : objet**

La présente annexe a pour objet de prendre en compte, pour l’exécution du contrat, la législation relative à la protection des données personnelles.

Les parties s’engagent à respecter, dans le cadre de l’exécution du présent contrat, les dispositions issues du règlement UE n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, le « Règlement Général sur la Protection des Données » ou « R.G.P.D. ») ainsi que la loi n°78-17 du 6 janvier 1978 modifiée (dite « loi informatique et libertés).

Pour l’interprétation de la présente annexe, il est rappelé que :

- l’expression « sous-traitant », au sens du R.G.P.D., désigne le Titulaire du marché public,

- l’expression « responsable de traitement », au sens du R.G.P.D., désigne le Pouvoir Adjudicateur.

**◼ Article 2 : Description du traitement de données pour lequel le Titulaire est sous-traitant**

Le Titulaire ne peut être amené à consulter ou à traiter des données à caractère personnel du Pouvoir Adjudicateur que dans le cadre de l’exécution des prestations prévues dans le contrat, dans les conditions décrites ci-après.

|  |  |
| --- | --- |
| **Description du traitement** | |
| Objet et finalités du traitement | *Aide à la rédaction : exemple pour un marché de maintenance informatique :*  *La finalité du traitement par le Titulaire est l’exécution des prestations de maintenance, objet du marché. Le traitement est réalisé uniquement aux fins de diagnostic des évènements signalés par le Pouvoir Adjudicateur et la réalisation des actions curatives correspondantes.* |
| Durée du traitement | La durée du traitement est limitée à la durée du marché public. |
| Catégories de personnes concernées et type de données traitées | *Aide à la rédaction : exemples des trois grandes typologies de données à caractère personnel traitées par le CHU (clause à personnaliser) :*  *• données à caractère personnel des patients du Pouvoir Adjudicateur : données de santé et données relatives à leur identité, collectées directement auprès des patients dans le cadre l’activité des professionnels de santé :*   * + - * Nom, prénom, date de naissance, sexe,       * Coordonnées (adresse, téléphone, courriel),       * Identifiants nationaux,       * Autres identifiants (numéro d'hôpital et/ou de séjour),       * Détails d'assurabilité nécessaires à la gestion des contrats de facturation,       * Données relatives à l’état de santé.   *• données relatives aux interlocuteurs extérieurs de l’établissement (médecins, professions médicales ou paramédicales, cliniques et leurs employés…) :*   * + - * Nom, prénom, genre, titre,       * Coordonnées (adresse, téléphone, télécopie, courriel),       * Numéro d'agrément,       * Numéro de service.   *• données relatives aux employés du Pouvoir Adjudicateur :*   * *Nom, prénom,*   + - * *Coordonnées* (adresse, téléphone, télécopie, courriel), * *Code ou numéro de service.* |
| Nature des opérations réalisées sur les données  (modalités de consultation ou de collecte des données, personnes amenées à manipuler les données, modalités de stockage ou de conservation des données, etc…) | *Aide à la rédaction :*  *Exemple pour un marché de maintenance de logiciel médical (clause à personnaliser) :*  *Le Titulaire ne procède à aucun traitement routinier de ces données mais sera inévitablement amenée à les visualiser de manière incidente dans l'exécution du contrat de maintenance (analyse et correction de problèmes) ainsi qu'au cours de projets d'implémentation (import initial du fichier patient, du fichier des utilisateurs du système et du fichier des prescripteurs).*  *Seule la visualisation de ces données de patients peut être rendue nécessaire dans le cadre de l'exécution du contrat de maintenance et de l'implémentation de projets. Elle se fera soit par un accès à distance sur le système implanté chez le Pouvoir Adjudicateur, en accord avec les règles de connexion convenues avec le Pouvoir Adjudicateur, soit lors de la présence sur site d'un employé du Titulaire. Ces interventions ne doivent jamais requérir la création de copies des données des patients et des médecins dans le système du Titulaire ainsi que les données des utilisateurs du système et ne doivent jamais requérir le moindre transfert de données à l’extérieur du système implanté chez le Pouvoir Adjudicateur.* |
| Mesures techniques et organisationnelles adoptées par le Titulaire afin de garantir un niveau de sécurité adapté au risque | *Aide à la rédaction :*  *Préciser les mesures techniques (authentification, sauvegarde, cryptage des données…) ou organisationnelles (politique d’accès aux données…) mises en place.*  *S’il s’agit d’un logiciel médical en mode SAAS ou plus généralement de tout marché impliquant une sortie de données patients en dehors du CHU (stockés sur les serveurs du Titulaire) vérifier et préciser impérativement :*  Le Titulaire ou son sous-traitant est **agréé ou certifié pour héberger des données de santé.**  Les données de santé doivent obligatoirement être stockées sur des **serveurs situés sur le territoire de l’Union Européenne** et ne faire l’objet d’aucun transfert hors U.E. |
| Sort des données en fin de contrat.  Délai de restitution et/ou de destruction des données. | *Aide à la rédaction :*  Cet article peut être sans objet si le Titulaire ne stocke aucune donnée à caractère personnel sur ses serveurs.  Dans le cas contraire, indiquer si les données sont détruites ou restituées au CHU ou transférées au nouveau Titulaire et sous quel délai. |

**◼ Article 3 : Obligations du Titulaire vis-à-vis du Pouvoir Adjudicateur dans le cadre de la sous-traitance du traitement**

#### Obligations générales du Titulaire vis-à-vis du Pouvoir Adjudicateur

Le Titulaire s'engage à :

1. traiter les données uniquement pour la durée du marché ;
2. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance ;
3. traiter les données conformément aux instructions documentées figurant dans le marché ;

Si le sous-traitant considère qu’une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l’Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l’Union ou du droit de l’Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

1. lorsque la nature du produit ou du service objet du marché le permet (notamment s’agissant des logiciels hébergés en interne), **à n'effectuer aucun transfert hors de l’établissement**, des données à caractère personnel concernant les patients, les employés ou les interlocuteurs extérieurs (médecins, cliniques, leurs employés…) du Pouvoir Adjudicateur auxquelles les personnels du Titulaire auraient accès, **et à ne réaliser en aucun cas, des copies de sauvegarde de ces données sur ses serveurs** ;
2. garantir la confidentialité et l’intégrité des données à caractère personnel traitées dans le cadre du présent marché ;
3. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché :

* s’engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
* prennent connaissance de la Politique de Sécurité des Systèmes d’Information (P.S.S.I.) du Pouvoir Adjudicateur ainsi que de la charte d’utilisation du Système d’Information à destination des Titulaires de profils à pouvoir, dans sa version en vigueur pendant l’exécution du marché ;

1. sous-traitance : le Titulaire peut faire appel à un sous-traitant pour mener des activités de traitement spécifiques à condition d’avoir sollicité préalablement l’accord du Pouvoir Adjudicateur, au moyen d’une notification écrite mentionnant les activités sous-traitées, l’identité et les coordonnées du sous-traitant et la durée du contrat de sous-traitance. Il incombe au Titulaire de s’assurer que le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du R.G.P.D. Le sous-traitant est tenu de respecter les obligations du présent contrat, pour le compte du responsable de traitement. Il appartient au Titulaire de s’assurer que son sous-traitant présente les mêmes garanties sus évoquées. Le Pouvoir Adjudicateur peut refuser par une décision expresse l’agrément d’un sous-traitant qui ne présenterait pas des garanties suffisantes en la matière. Le Titulaire demeure pleinement responsable, devant le Pouvoir Adjudicateur, de l’exécution de ses obligations par son sous-traitant.

#### Exercice de leurs droits par les personnes concernées

Il appartient au Pouvoir Adjudicateur de fournir, au moment de la collecte de données, l’information aux personnes concernées par les opérations de traitement qu’il réalise. La formulation et le format de l’information sont définis par le Pouvoir Adjudicateur.

Dans la mesure du possible, le Titulaire doit aider le Pouvoir Adjudicateur à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées : droit d’information, d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du Titulaire des demandes d’exercice de leurs droits, le Titulaire doit adresser ces demandes dès réception par courrier électronique à [dpo@chu-toulouse.fr](mailto:dpo@chu-toulouse.fr).

#### Notification des violations de données à caractère personnel

Le sous-traitant notifie au Pouvoir Adjudicateur toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance à l’adresse suivante : [dpo@chu-toulouse.fr](mailto:dpo@chu-toulouse.fr). Cette notification est accompagnée de toute documentation utile afin de permettre au Pouvoir Adjudicateur, si nécessaire, de notifier cette violation à la Commission Nationale Informatique et Libertés (C.N.I.L.).

#### Mesures de sécurité

Le Titulaire s’engage à mettre en œuvre les mesures de sécurité appropriées et adaptées au risque, telles que prescrites par le présent avenant parmi celles listées à l’article 32 du R.G.P.D., notamment par la mise en place de procédure de sauvegarde et d'authentification, et l’application, s’agissant de ses outils, produits, applications ou services, des principes de protection des données dès la conception et de protection des données par défaut tels que définis par l’article 25 du R.G.P.D. ;

Le Titulaire est réputé se conformer à ses obligations en matière de sécurité, s’il indique avoir élaboré un code de bonne conduite adopté sur le fondement de l’article 40 du R.G.P.D. ou bénéficier d’une certification accordée sur le fondement de l’article 42 du R.G.P.D.

#### Registre des catégories d’activités de traitement

Le sous-traitant doit tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du Pouvoir Adjudicateur comprenant l’ensemble des éléments listés à l’article 30 du R.G.P.D.

#### Assistance du Titulaire vis-à-vis du Pouvoir Adjudicateur

Le cas échéant, le Titulaire assiste le Pouvoir Adjudicateur pour la réalisation d’analyses d’impact relative à la protection des données ainsi que pour la réalisation de la consultation préalable de l’autorité de contrôle.

#### Documentation

Le Titulaire met à la disposition du Pouvoir Adjudicateur la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le Pouvoir Adjudicateur ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

#### Sort des données en fin de contrat

Au terme de la prestation, si l’objet du contrat nécessite que le Titulaire stocke des données à caractère personnel sur ses serveurs ou ceux de ses sous-traitants dans les conditions décrites ci-avant, il s’engage à renvoyer toutes ces données au Pouvoir Adjudicateur ou au nouveau Titulaire du marché, en fonction des instructions convenues entre les parties dans le présent avenant ou ultérieurement. Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du Titulaire. Une fois détruites, le Titulaire doit justifier par écrit de la destruction.

**◼ Article 4 : Obligations du Pouvoir Adjudicateur dans le cadre de la sous-traitance du traitement**

#### Obligations générales

Le Pouvoir Adjudicateur s’engage à :

1. Informer les patients de leurs droits consultatifs, des durées légales minimales de conservation et des mesures de sécurité apportées à la gestion de leurs données cliniques ;
2. Veiller à l'accomplissement de toutes formalités, de l'obtention de toutes autorisations, et de la mise en œuvre toutes obligations légales ou réglementaires en découlant, y compris déclaratives, de tenue de registres, de notifications ou d'informations, d'analyses d'impact, de consultation préalable des autorités de protection des données à caractère personnel ;
3. A veiller à ce que son personnel, ainsi que les Titulaires d’autres marchés publics, pouvant intervenir sur les données personnelles objet du contrat, respectent ces dispositions ;
4. A prendre toutes mesures techniques et organisationnelles nécessaires à la sécurité du traitement.

#### Obligations vis-à-vis du Titulaire

Le Pouvoir Adjudicateur s’engage à :

1. Fournir au Titulaire les données nécessaires pour permettre le traitement objet du marché ;
2. Documenter par écrit toute instruction concernant le traitement des données par le Titulaire ;
3. Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le R.G.P.D. de la part du Titulaire ;
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire.

|  |
| --- |
| **E - Signature du Titulaire du marché ou de l’accord-cadre** |

|  |  |  |
| --- | --- | --- |
| **Nom, prénom et qualité**  **du signataire (\*)** | **Lieu et date de signature** | **Signature** |
|  |  |  |
|  |  |  |
|  |  |  |

*NOTA :*

*La signature doit être originale. Le signataire doit avoir le pouvoir d’engager la personne qu’il représente.*

|  |
| --- |
| **F - Signature du Pouvoir Adjudicateur** |

**Pour le CHU de Toulouse :**

A : …………………… , le #date#

Signature

Le Directeur général

#signature#